

CLAIMS

*Pub
al 1*

1. A system for delivering institutional data to a customer, comprising:

an institutional server, wherein the institutional server includes a system for separately serving a first database containing private data and a second database containing public data;

a service provider, wherein the service provider includes a system for receiving an encrypted version of the private data and an unencrypted version of the public data; and

a client, wherein the client includes a system for displaying a merged version of the private and public data.

2. The system of claim 1, wherein the client includes a mechanism for decrypting the encrypted private data.

3. The system of claim 1, further comprising a system for making the customer anonymous to the service provider.

4. The system of claim 3, wherein the system for making the customer anonymous to the service provider includes a mechanism for determining a service level available to the customer.

5. The system of claim 1, wherein the service provider includes a system for analyzing the use of the public data by the customer without knowing an identity of the customer.

1 6. The system of claim 1, wherein the merged version of the private and public data is
2 downloaded to the client by the service provider.

1 7. The system of claim 1, wherein the private and public data are downloaded to the client by
2 the institutional server and service provider, respectively.

1 8. The system of claim 1, wherein the encrypted version of the private data is encrypted
2 using a public key infrastructure protocol.

1 9. The system of claim 1, wherein the client includes an interface that can be customized into
2 a first window for viewing the public data and a second window for viewing the private data.

1 10. A method of preserving privacy between a customer and an institution in a computer
2 network environment, comprising the steps of:

3 separating data associated with the institution into a first database of private data and
4 a second database of public data;

5 storing an encrypted copy of the private data and an unencrypted copy of the public
6 data with an intermediary service provider;

7 providing to the customer a security system that allows the customer to decrypt the
8 encrypted data and remain anonymous to the intermediary service provider;

9 merging the encrypted copy of the private data and the unencrypted copy of the public
10 data; and

11 providing an interface that allows the customer to view the merged data.

1 11. The method of claim 10, wherein the security system includes a public key infrastructure
2 protocol.

1 12. The method of claim 10, comprising the further step of customizing the interface to
2 include a first window for viewing the public data and a second window for viewing the
3 private data.

1 13. The method of claim 10, wherein the public data includes data available externally to the
2 institution.

1 14. A method of preserving privacy between a customer and an institution in a computer
2 network environment, comprising the steps of:

3 separating data associated with the institution into a first database of encrypted private
4 data and a second database of public data;

5 loading an unencrypted copy of the public data to a service provider;

6 loading to a client the encrypted private data from the institution and the unencrypted
7 copy of the public data from the service provider;

8 providing to the customer a security mechanism that allows the customer to decrypt
9 the encrypted data and remain anonymous to the service provider; and

10 providing an interface that allows the customer to view the encrypted copy of the
11 private data and the unencrypted copy of the public data.

1 15. The method of claim 14, wherein the security mechanism includes a public key
2 infrastructure protocol.

1 16. The method of claim 14, comprising the further step of customizing the interface to
2 include a first window for viewing the public data and a second window for viewing the
3 private data.

1 17. The method of claim 14, wherein the public data includes data available externally to the
2 institution.

1 18. A program product stored on a recordable medium that when executed, preserves privacy
2 between a customer and an institution in a computer network environment, comprising:

3 a system for separating data associated with the institution into a first database of
4 encrypted data and a second database of unencrypted data;

5 a system for providing a copy of the second database of unencrypted data to an
6 intermediary service provider;

7 an interface that allows the customer to view the first database of encrypted data and
8 the copy of the second database of unencrypted data provided to the intermediary service
9 provider; and

10 a security system that allows the customer to decrypt the encrypted data and remain
11 anonymous to the intermediary service provider.

1 19. The program product of claim 18, further comprising:

2 a system for providing a copy of the first database of unencrypted data to the
3 intermediary service provider.